

REMARKS

Claim 1-28 are pending in the present application, and all claims stand rejected under 103 for various combinations of cited references. For at least the reasons set forth below, Applicant respectfully traverses these rejections.

No Official Notice Taken

In several places, the Examiner appears to have relied upon personal, subjective knowledge, rather than teaching of the cited art. For example, in the paragraph spanning pages 4 and 5, the Examiner stated "it is well known in the art ...". Likewise, in the paragraph spanning pages 5 and 6, the Examiner stated "It is common practice ...". Similarly, in the third paragraph on page 8, the Examiner alleged that Jenkins' hash function "is faster and more efficient than the one you are using now." In addition, in the second paragraph on page 10, the Examiner alleged "it is well known in the art that an easy way to include two pieces of data in one message is to concatenate the two pieces of data together."

The foregoing are examples of conclusions that are set forth in the Office Action, without providing any supporting citations. Therefore, the conclusions appear to be based solely on the personal, subjective knowledge of the Examiner. As such, the underlying rejections are improper, and for at least this reason, the rejections based on these assertions should be withdrawn. Nowhere does the Examiner take "Official Notice" of any of these alleged facts. Consequently, the undersigned need not reply with a specific, evidentiary traversal of a taking of Official Notice. Should the Examiner intend to take Official Notice of any of these allegations, then such notice should be properly set out in an ensuing, non-FINAL Office Action.

In an effort to advance the prosecution of this application (in the event that the Examiner intends on taking Official Notice of one or more of these allegations), the undersigned provides the following excerpt from a recent decision by the Court of Appeals for the Federal Circuit, in which the Federal Circuit vacated and remanded a decision of the Board of Patent Appeals, which had upheld an improper taking of Official Notice by an Examiner. There, the Federal Circuit stated:

The rationale supporting an obviousness rejection may be based on common knowledge in the art or "well-known" prior art. The examiner may take official notice of facts outside of the record which are capable of instant and unquestionable demonstration as being "well-known" in the art. *In re Ahlert*, 57 C.C.P.A. 1023, 424 F.2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970) ...

...
When a rejection is based on facts within the personal knowledge of the examiner, the data should be stated as specifically as possible, and the facts must be supported, when called for by the applicant, by an affidavit from the examiner. Such an affidavit is subject to contradiction or explanation by the affidavits of the applicant and other persons. See 37 CFR 1.104(d)(2).

...
For further views on official notice, see *In re Ahlert*, 57 C.C.P.A. 1023, 424 F.2d 1088, 1091, 165 USPQ 418, 420-421 (CCPA 1970) ("[A]ssertions of technical facts in areas of esoteric technology must always be supported by citation of some reference work" and "allegations concerning specific 'knowledge' of the prior art, which might be peculiar to a particular art should also be supported."

...
MPEP § 2144.03 (7th ed.1998) (*emphases added*); see also MPEP § 2144.03 (7th ed., rev.1, 2000). Certainly, the relative speed advantages of CAMs vis-à-vis "bitmap memories" and the feasibility of substituting one for the other can hardly be described as a fact that is of "instant and unquestionable demonstration" for the purpose of taking official notice unsupported by any citation.

The record reflects that the examiner and the Board have managed to find motivation for substituting one type of memory for another without providing a citation of any relevant, identifiable source of information justifying such substitution. The statements made by the Examiner, upon which the Board relied, amount to no more than conclusory statements of generalized advantages and convenient assumptions about skilled artisans. At least under the MPEP then in effect, such statements and assumptions are inadequate to support a finding of motivation, which is a factual question that cannot be resolved on "subjective belief and unknown authority." *Lee*, 277 F.3d at 1344. Under such circumstances, with respect to core factual findings, "the Board must point to some concrete

evidence in the record in support" of them, rather than relying on its assessment of what is "well recognized" or what a skilled artisan would be "well aware." In re Zurko, 258 F.3d 1379, 1385-86 (Fed.Cir.2001). "To hold otherwise would render the process of appellate review for substantial evidence on the record a meaningless exercise." *Id.* at 1386 (citing Baltimore & Ohio R.R. Co. v. Aberdeen & Rockfish R.R. Co., 393 U.S. 87, 91-92, 89 S.Ct. 280, 21 L.Ed.2d 219 (1968)).

The PTO, perhaps realizing the deficiencies in the record in this regard, provides numerous citations in its brief to specific passages in Pieters, Belser, and Doyle in a valiant attempt to muster substantiation for the Board's findings. We cannot consider such post hoc attempts at bolstering the record in our review for substantial evidence. Burlington Truck Lines, Inc. v. United States, 371 U.S. 156, 168, 83 S.Ct. 239, 9 L.Ed.2d 207 (1962) ("[C]ourts may not accept appellate counsel's post hoc rationalization for agency action."). Our review must be limited to those grounds relied on and articulated by the Board; otherwise, the applicant may be deprived of a fair opportunity to support his position. See *Lee*, 277 F.3d at 1345; see also SEC v. Chenery Corp., 332 U.S. 194, 196, 67 S.Ct. 1575, 91 L.Ed. 1995 (1947) ("[T]he court is powerless to affirm the administrative action by substituting what it considers to be a more adequate or proper basis.").

In re Beasley, 117 Fed.Appx. 739 (Fed. Cir. 2004).

Applicant traverses all rejections of the Examiner. In this response, Applicant focuses its traversals on the independent claims. However, the lack of specific attention given to certain dependent claims should not be viewed as any admission or agreement with positions taken by the Examiner with respect to those claims. Indeed, as the Examiner has not taken Official Notice with regard to any of these positions, no specific or evidentiary traversal by the Applicant is required.

Independent claims 1, 17, and 21

The present application contains three independent claims: claims 1, 17, and 21. The Office Action has rejected each of these claims under 35 U.S.C. § 103(a) as allegedly unpatentable over the combination of U.S. patent 6,374,359 to Shrader in view of U.S. published

application 2003/0110399 to Rail and further in view of U.S. patent 5,586,185. For at least the following reasons, Applicant disagrees.

As an initial matter, Applicant notes that the Office Action has set forth a single rejection (pages 2 and 3) as applying to all of claims 1, 17, and 21. Applicant submits that each of these claims defines differing subject matter, and that a rejection should address each claim individually. The following response will focus on independent claim 1. For at least the reasons set forth below, the rejection of independent claim 1 should be withdrawn.

Independent claim 1 recites:

1. A method for authenticating a Web session comprising:
receiving a user ID; computing a message digest of the user ID;
computing an expiration timestamp for the session;
selecting an index number;
combining the message digest and expiration timestamp;
accessing an encryption key using the index number;
encrypting the combined message using the accessed encryption key;
and
converting the encrypted message into an ASCII string.

(*Emphasis added.*) Applicant respectfully submits that claim 1 patently defines over the cited art for at least the reason that the cited art fails to disclose the features emphasized above.

The undersigned submits that there are a number of distinctions in the embodiment of claim 1, but several features are particularly distinctive over the cited art. In addition, the undersigned respectfully submits that the Office Action has taken an overly expansive view of certain claim features in forming the rejection.

For example, as emphasized above, claim 1 defines elements of: “selecting an index number,” “accessing an encryption key *using the index number*,” and “*encrypting the combined message using the accessed encryption key*.” In applying the principal reference (Shrader), the Office Action states that Shrader teaches “encrypting a message using an encryption key.”

However, this application of Shrader does not address the claimed features of selecting an index number, using that number to access an encryption key, and then using the encryption key to encrypt a combined message.

Indeed, the Office Action later admits that the combination of Shrader and Rail “fail to specify: selecting an index number; accessing an encryption key using the index number; and encrypting the message using the accessed encryption key.” Instead, the Office Action relies upon Shibata for allegedly teaching these features. Applicant disagrees. In fact, unlike the present invention (which is directed to systems and methods for authenticating Web sessions), Shibata is directed to a system and method for transmitting and receiving encrypted information to apparatus, such as a telephone, radio communication equipment, or a facsimile machine (see col. 1, lines 8-11). There is no teaching or suggestion, anywhere within Shibata, of the Internet or the World Wide Web, much less the authentication of a Web session. As such, the undersigned submits that Shibata is wholly unrelated to the claimed invention, and certainly a person would not be motivated to combine select teachings from Shibata with Shrader and Rail. For at least this reason, the rejection of claim 1 should be withdrawn.

Further, with regard to the above-quoted elements, the Office Action has relied upon the teachings of col. 10, lines 43-51 and col. 18, lines 54-64 of Shibata as allegedly teaching these features. In fact, these cited portions of Shibata actually state:

The numeric keys 21 are used for entering numeric values such as facsimile numbers, cipher numbers, cipher key number and simplified facsimile numbers. They serve as index number input means for entering index numbers, or cipher numbers, in the user terminal table and cipher key table, cipher key input means for entering cipher key numbers in the cipher key table, and operation number input means for entering operation numbers or simplified facsimile numbers.

...

Subsequently, it is judged whether the facsimile machine is set to cryptographic communications mode (Step S73). If cryptographic

communications mode is activated (YES in Step S73), the outgoing data is encrypted by a predefined encryption algorithm by using the cipher key corresponding to the specified cipher number (Step S74) and transmitted to the recipient's facsimile machine 14 via the data transfer block 5 and telephone line 13 (Step S75). If cryptographic communications mode is not activated (NO in Step S73), the outgoing data is transmitted without encryption to the recipient's facsimile machine 14 (Step S75).

Applicant respectfully submits that these cited portions of Shibata fail to properly teach or disclose the claimed features emphasized above. For example, the above-quoted portion references an "index number." However, there is no disclosure of this "index number" being used to access an encryption key, as expressly claimed in claim 1. In addition, the above-quoted portion of Shibata fails to teach or disclose encrypting a "combined message" (the combined message comprising both a message digest and expiration timestamp) using the accessed encryption key. For at least these reasons, Applicant respectfully submits that claim 1 patently defines over the teachings of Shibata and the rejection of claim 1 should be withdrawn.

As a separate and independent basis for the patentability of claim 1, the Office Action admitted that the primary reference (Shrader) failed to disclose the computation of an expiration timestamp. Instead, the Office Action cites paragraph 0032 of Rail as allegedly disclosing this feature. Applicant disagrees. Paragraph 0032 of Rail is describing a portion of a Web server that is determining whether a passkey has expired. As described in Rail, a passkey is a non-persistent cookie. A passkey integrity tool is described, which determines a time period that has elapsed since the creation of the passkey. If more than an allowable time period has expired, then the passkey is deleted (see FIG. 3).

In contrast, claim 1 defines the computation of an expiration timestamp, and that the expiration timestamp forms part of a combined message that is encrypted and converted into an ASCII string. First, Rail fails to disclose the computation of a timestamp, as required by claim 1

(simply determining whether too much time has elapsed since the creation of a passkey is not the same as the computation of an expiration of a timestamp). More significantly, Rail fails to disclose the integration of an expiration timestamp into a combined message (and therefore fails to disclose the integration a combined message, which is further encrypted and converted into an ASCII string).

These are fundamental shortcomings of Rail (in the context for which it is cited), and for at least these additional reasons, the rejection of claim 1 should be withdrawn.

As a separate and independent basis for the patentability of claim 1, Applicant respectfully submits that the Office Action has failed to cite a proper suggestion or motivation for combining Shrader, Rail, and Shibata. In combining Rail with Shrader, the Office Action stated only that it would have been obvious “to form the device of Shrader et al using the methods of Rail for the added securities of knowing the cookie has not been tampered with (message digest) and the cookie is not being used after a given length of time has elapsed (timestamp).” (Office Action p. 3). The embodiment of claim 1 has nothing to do with cookies, so this assertion by the Office Action appears misplaced. As the Federal Circuit has made clear, “both the suggestion and the expectation of success must be founded in the prior art, not in the applicant's disclosure. W. L. Gore & Associates, Inc. v. Garlock Thomas, Inc., 721 F.2d 1540, 1551 (Fed. Cir. 1983).

Further, in combining Shibata with Shrader and Rail, the Office Action alleged (see p. 3) “Shibata et al. meets [the qualifications of Shrader and Rail] and teaches improved key management through ‘a cipher key table’ in which a plurality of cipher keys and their index numbers are updatably registered.” It is not clear what the Office Action means by “Shibata meets these qualifications...” Notwithstanding this uncertainty, this alleged motivation is clearly

improper in view of well-established Federal Circuit precedent. In this regard, the showing of combinability must nevertheless be "clear and particular." Dembiczak, 175 F.3d at 999, 50 USPQ2d at 1617. Significantly, where there is no apparent disadvantage present in a particular prior art reference, then generally there can be no motivation to combine the teaching of another reference with the particular prior art reference. Winner Int'l Royalty Corp. v. Wang, No 98-1553 (Fed. Cir. January 27, 2000).

The Office Action alleged that the combination would have been obvious because "Shibata et al. meets [the qualifications of Shrader and Rail] and teaches improved key management through 'a cipher key table' in which a plurality of cipher keys and their index numbers are updatably registered." This allegation, however, fails to point to specific teachings that would lead one skilled in the art to combine them in the manner relied upon by the Office Action to form the rejections. Consequently, the alleged motivations to combine are not teachings from the prior art itself, but rather mere conjecture by the Office Action and are thus improper.

Accordingly, for at least the additional reason that the Office Action failed to identify proper motivations or suggestions for combining the various references to properly support the rejection of claim 1 under 35 U.S.C. § 103, those rejections should be withdrawn.

As the Office Action has not separately or independently addressed claim 17 or 21, Applicant does not separately address these claims in this response. As the Office Action rejected these claims on a collective basis with claim 1, Applicant submits that these claims should be allowed with claim 1. Applicant does note, however, that each of these claims is

patently distinct from claim 1, and that any continued rejection of these claims should be set forth in an ensuing (non-Final) Office Action, separate and apart from any rejection of claim 1.

Dependent Claims

Claims 2-16, 18-20, and 22-28 depend from independent claims 1, 17, and 21, respectively and patently define over the cited art for at least the same reasons that these claims contain all limitations of the base claims from which they depend.

AUTHORIZATION TO DEBIT ACCOUNT

It is believed that no extensions of time or fees for net addition of claims are required, beyond those which may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required therefor (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Company's deposit account no. 08-2025.

Respectfully submitted,



Daniel R. McClure
Registration No. 38,962

(770) 933-9500

Please continue to send all future correspondence to:

Hewlett-Packard Development Company, L.P.
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400